ABSTRACT OF THE DISCLOSURE

A secure mail transmission system provides virus protection, document tracking, tamper proofing, authentication through digital signatures in addition to secure encryption means and time date verification for e-mail messages. The system encrypts a sent message at a user station and provides digital authentication and confidential encryption schemes prior to delivery of the secure mail message to the secure mail system over a communication network. The secure mail system unpacks the secure transmission, verifies the contents, provides a time date stamp and virus checking before reencrypting an retransmitting the original message. The transmission can be logged and stored for later verification. The recipient of the secure message can be a subscriber or non-subscriber and can use supported e-mail platforms, unsupported e-mail platforms, or unknown e-mail systems and receive the secured message with little or no variation from their typical application interface usage. The system provides secure features including the use of public/private key pairs, hashing algorithms and digital signatures to provide privacy and authentication of the secure mail messages. The private key associated with an individual user need not be stored anywhere. The system permits secure and private electronic communications with virus checking and return receipt notifications available.